

CLAIMS

J. O. B. J. E. M. 1900

100-1474-022602
said memory area operation unit; and,

under the control of the memory area operation unit, providing the encrypted second module data to the integrated circuit, decrypting the second module data by 5 using the first area management key data in the integrated circuit, decrypting the first module data in the decrypted second module by using the key data for dividing, and dividing the memory area to a first memory area to be used for service of the first service provider 10 and a second memory area to be used for service of the second service provider by using the second area management key data obtained by the decrypting.

2. A data processing method as set forth in claim 1, further comprising the step of having the integrated 15 circuit divide the memory area into the first memory area wherein at least one of a write operation of data and a rewrite operation of data is authorized on the condition that the first area management key data is used and the second memory area wherein at least one of a write 20 operation of data and a rewrite operation of data is authorized on the condition that the second area management key data is used.

3. A data processing method as set forth in claim 1, further comprising:
25 having the integrated circuit further store

first system key data and authorize at least one of a write operation of data to the memory area and a rewrite operation of data in the memory area on the condition the first system key data and the first area management key

5 data are used;

having the memory area operation unit encrypt first module data further including second system key data by the key data for dividing and provide the same to the first service provider;

10 having the first service provider encrypt second module data including the encrypted first module and division condition information indicating the condition for dividing the memory area for use by another service provider by using the first area management key

15 data and provide it to the memory area operation unit; and

having the integrated circuit decrypt the second module data by using the first area management key data, decrypt the first module data in the decrypted

20 second module by using the key data for dividing, and divide the memory area by using the second system key data, second area management key data, and division condition information obtained by the decrypting.

4. A data processing method as set forth in claim

25 1, further comprising

providing a memory area division apparatus for dividing said memory area to said second service provider under the control of said memory area operation unit and having said memory area division apparatus

5 provide said encrypted second module data to said integrated circuit.

5. A data processing method as set forth in claim
2, when a plurality of third memory areas can be defined
in said second memory area and third area management key
10 data used for performing at least one of a write
operation of data to the third memory area and a rewrite
operation of data in the third memory area is defined for
each of said plurality of third memory areas.

15 further comprising the steps of having
said memory area operation unit encrypt third
area management key data by second area management key
data and provide the same to said memory area division
apparatus:

having said memory area division apparatus

20 provide said encrypted third area management key data to
said integrated circuit; and

having said integrated circuit decrypt said encrypted third area management key data by using said second area management key data, establish correspondence with said third memory areas defined in said second

九月九日憶山東兄

memory area to store said third area management key data obtained by said decrypting.

6. A data processing method as set forth in claim 5, further comprising the step:

5 having said memory area operation unit assign a service code for identifying a service provided by using the third memory area for each of said third memory areas and generate and store an area code list indicating an area code for identifying said third memory area, said 10 third area management key data corresponding to the third memory area, and said service code assigned to the third memory area in correspondence.

7. A data processing method as set forth in claim 3, further comprising the steps of:

15 providing a memory area division apparatus for dividing said memory area to said second service provider under the control of said memory area operation unit;

having said memory area division apparatus provide said encrypted second module data to said 20 integrated circuit;

having said memory area operation unit provide first degenerate key data obtained by encrypting by using said second system key data and said second area management key data to said memory area division 25 apparatus;

having said integrated circuit generate second degenerate key data by encrypting by using said second system key data obtained by decrypting and said second area management key data; and

5 performing mutual authentication between said memory area division apparatus and said integrated circuit by using said first degenerate key data and said second degenerate key data.

8. A data processing method as set forth in claim
10 6, further comprising the steps of:

having said memory area operation unit provide an operation file registration apparatus to said second service provider,
provide said third area management key data to
15 said operation file registration apparatus, and establish correspondence between said service code in said area code list and said area code to provide the same to said operation file registration apparatus;

having said operation file registration apparatus store file registration permission data indicating said service code and file management key data issued by said second service provider in correspondence, encrypt said file registration permission data by using said third area management key data, and provide the same
25 to said integrated circuit; and

having said integrated circuit decrypt said
file registration permission data by using said third
area management key data and write file data relating to
a service of said second service provider to said third
5 memory area by using said file management key data in
said decrypted file registration permission data.

9. A data processing method as set forth in claim
4, further comprising the steps of,

when there are a plurality of said first
10 service providers, and said first system management key
data and a system code for identifying said first service
provider are added to each of said plurality of first
service providers,

15 having said memory area operation unit
receive rejection information for specifying a
party for which provision of services from respective
service providers by using the same integrated circuit is
rejected from said first service provider and said second
service provider,

20 generate a registerable system code list
indicating said system code added to said first service
provider capable of providing a service by said same
integrated circuit as said second service provider based
on said rejection information, and

25 provide the registerable system code list to

said memory area division apparatus; and

having said memory area division apparatus
judge whether or not to divide said memory area of the
integrated circuit based on said system code stored in
5 the integrated circuit and said registerable system code
list before dividing said memory area of said integrated
circuit.

10. A data processing method as set forth in claim
1, further comprising the step of having said memory area
10 operation unit pay a fee for using said second memory
area of said integrated circuit to said first service
provider.

11. A data processing method as set forth in claim
1, further comprising the step of having said second
15 service provider pay a fee for using said second memory
area of said integrated circuit to said memory area
operation unit.

12. A data processing method as set forth in claim 1, wherein said portable device is a card.

20 13. A data processing system for processing so that
a portable device mounting an integrated circuit storing
key data for dividing and first area management key data
which is authorized to perform at least one of a write
operation of data to a memory area of said integrated
25 circuit and a rewrite operation of data to the memory

area on the condition that the first area management key data is used makes a second service provider provide a service using part of said memory area of said integrated circuit when issued by a first service provider providing a service using said memory area, wherein the system has 5 a memory area operation processing apparatus used by a memory area operation unit which manages the key data for dividing,

10 a first service provider processing apparatus used by the issuer of the portable device which is the first service provider, and

15 a second service provider processing apparatus used by the first service provider;

20 wherein:

the memory area operation processing apparatus encrypts first module data including second area management key data by the key data for dividing and sends the same to the first service provider processing apparatus;

25 the first service provider processing apparatus encrypts second module data including the received encrypted first module by using the first area management key data and sends the same to the memory area operation processing apparatus;

30 the memory area operation processing apparatus

THE JOURNAL OF CLIMATE

provides the received encrypted second module data to the integrated circuit; and

the integrated circuit decrypts the second module data by using the first area management key data, 5 decrypts the first module data in the decrypted second module by using the key data for dividing, and divides the memory area to a first memory area to be used for service of the first service provider and a second memory area to be used for service of the second service provider by using the second area management key data obtained by the decrypting under control of the memory 10 area operation unit.

14. A data processing system as set forth in claim
13, wherein said integrated circuit divides said memory
area to said first memory area wherein at least one of a
write operation of data and a rewrite operation of data
is authorized on the condition that said first area
management key data and said second memory area are used
wherein at least one of a write operation of data and a
rewrite operation of data is authorized on the condition
20 that said second area management key data is used.

15. A data processing system as set forth in claim
13, wherein:

25 system key data and authorizes at least one of a write
said integrated circuit further stores first

operation of data to said memory area and a rewrite operation of data in the memory area on the condition that said first system key data and said first area management key data are used;

5 said memory area operation processing apparatus
 encrypts first module data further including second
 system key data by said key data for dividing and
 provides the same to a first service provider processing
 apparatus:

10 said first service provider processing
apparatus encrypts second module data including said
encrypted first module and division condition information
indicating conditions of dividing said memory area for
use of other service providers and provides it to said
15 memory area operation unit processing apparatus; and

20 said integrated circuit decrypts said second module data by using said first area management key data, decrypts said first module data in the decrypted second module by using said key data for dividing, and divides said memory area by using said second system key data, second area management key data, and said division condition information obtained by the decrypting.

16. A portable device mounting an integrated circuit used for a first service provider providing a service, wherein the integrated circuit comprises:

A00000000000000000000000000000000

 a memory means for storing key data for
 dividing managed by a memory area operation unit
 performing processing to make a second service provider
 provide a service using a part of a memory area of the
5 integrated circuit and first area management key data;
 an input means for inputting a module including
 second area management key data issued by the memory area
 operation unit which is encrypted by the memory area
 operation unit by using the key data for dividing and
10 furthermore encrypted by the first service provider by
 using the first area management key data; and
 a processing means for decrypting the input
 module by using the key data for dividing and the first
 area management key data, dividing a memory area of the
15 memory means to a first memory area and a second memory
 area by using the second area management key data in the
 decrypted module, authorizing at least one of a write
 operation of data to the first memory area and a rewrite
 operation of data in the memory area on the condition
20 that the first area management key data is used and
 authorizing at least one of a write operation of data to
 the second memory area and a rewrite operation of data in
 the memory area on the condition that the second area
 management key data is used.
25 17. A portable device as set forth in claim 16,

wherein said processing means authorizes a write operation of a file used for processing of the processing means in said first memory area on the condition that said first area management key data is used and 5 authorizes a write operation of a file used for processing of the processing means in said second memory area on the condition that said second area management key data is used.

18. A portable device as set forth in claim 16,

· said memory means further stores first system
key data;

said input means receives as input said module
further including second system key data; and

15 said processing means uses said second system
key data and said second area management key data in said
decrypted module to divide the memory area of said memory
means to said first memory area and said second memory
area, authorizes at least one of a write operation of
20 data to said first memory area or a rewrite operation of
data in the memory area on the condition that said first
system key data and said first area management key data
are used, and authorizes at least one of a write
operation of data to said second memory area or a rewrite
25 operation of data in the memory area on the condition

that said second system key data and said second area management key data are used.

19. A data processing apparatus for processing so that a portable device mounting an integrated circuit 5 storing distribution key data, a system code for identifying a first service provider, and first area management key data which is authorized to perform at least one of a write operation of data to a memory area of said integrated circuit and a rewrite operation of 10 data to the memory area on the condition that the first area management key data is used makes a second service provider provide a service using part of said memory area of said integrated circuit when issued by a first service provider providing a first service using said memory 15 area, wherein

the apparatus has a memory means, processing means, and input/output means;

the memory means stores rejection information for specifying a service provider which can provide 20 service by the same integrated circuit indicated by the first service provider and the second service provider;

the processing means encrypts a first module including second management key data by using the key data for dividing;

25 the input/output means outputs the encrypted

first module to provide it to the first service provider, receives as input a second module including the encrypted first module and encrypted in the first service provider by using the first area management key data, and outputs

5 the second module to provide it to a memory area division apparatus for dividing the memory area under control of the second service provider so that a part of the memory area of the integrated circuit can be used by the second service provider;

10 the processing means generates a registerable system code list indicating the system code added to the first service provider which can provide service by the same integrated circuit as the second service provider based on the rejection information; and

15 the input/output means outputs the system code list to provide it to the memory area division apparatus.

20. A data processing apparatus as set forth in claim 19, wherein

when said memory area division apparatus

20 divides said memory area of said integrated circuit to said first memory area wherein at least one of a write operation of data and a rewrite operation of data is authorized on the condition that said first area management key data is used and said second memory area

25 wherein at least one of a write operation of data and a

rewrite operation of data is authorized on the condition
that said second area management key data is used:

5 said processing means defines a plurality of
memory areas in said second memory area, issues third
area management key data used for performing at least one
of a write operation of data to the third memory area and
a rewrite operation of data in said third memory area for
each of said plurality of third memory areas and encrypts
the third area management key data by said second area
10 management key data; and

third area management key data to provide it to said memory area division apparatus.

21. A data processing apparatus as set forth in
15 claim 20, wherein said processing means issues a service
code for identifying a service provided by using the
third memory area for each of said third memory areas and
generates an area code list indicating an area code for
identifying said third memory areas, said third area
20 management data corresponding to the third memory area,
and said service code assigned to the third memory area
in correspondence; and

said memory means stores said area code list.

22. A data processing apparatus as set forth in
25 claim 21, wherein said input/output means establishes

correspondence between said area code included in said area code list and said service code and outputs the same to provide it to a file registration apparatus for writing file data used for a service of said second 5 service provider in said third memory area of said integrated circuit.

23. A data processing apparatus for processing so that a portable device mounting an integrated circuit storing distribution key data, a system code for 10 identifying a first service provider, and first area management key data which is authorized to perform at least one of a write operation of data to a memory area of said integrated circuit and a rewrite operation of data to the memory area on the condition that the first 15 area management key data is used makes a second service provider provide a service using part of said memory area of said integrated circuit when issued by a first service provider providing a first service using said memory area, wherein

20 the apparatus has a memory means, input/output means, and processing means;

the memory means stores a module including second area management key data issued by a memory area operation unit for managing processing of the data 25 processing apparatus and encrypted by the memory area

operation unit by using the key data for dividing and a registerable system code list indicating the system code added to the first service provider which can provide service by the same integrated circuit as the second 5 service provider;

the input/output means receives as input the system code from the integrated circuit; and

the processing means outputs the module to the integrated circuit via the input/output means when it 10 judges that the input system code is indicated in the registerable system code list.

24. A data processing apparatus for performing processing to write file data in a second memory area of an integrated circuit having a first memory area wherein 15 at least one of a write operation and rewrite operation of file data used for providing a first service is authorized on the condition that first area management key data is used and a second memory area wherein at least one of a write operation and rewrite operation of 20 file data used for providing a second service is authorized on the condition that second area management key data is used,

when a plurality of third memory areas are defined in the second memory area, third memory 25 management key data used for performing at least one of a

write operation of data to a third memory area and a rewrite operation of data in the third memory area is defined for each of the plurality of third memory areas, and said integrated circuit stores said third area

5 management key data; comprising,

 said data processing apparatus, comprising:

 a memory means storing third area management data and file key data which is issued by the second service provider, used at the time of writing the file 10 data to a third memory area, and encrypted by the third area management key data;

 an output means for outputting the encrypted file key data to the integrated circuit; and

 a writing means for writing file data to be 15 used for providing the second service to the second memory area of the integrated circuit by using the file key data.

25. A portable unit issuing method comprising the steps of:

20 issuing a portable unit mounting an integrated circuit storing key data for dividing and first area management key data and authorizing at least one of a write operation of data to a memory area in said integrated circuit and a rewrite operation of data in the 25 memory area on the condition that the first area

TOP SECRET - SOURCE CODE

management key data is used and

requesting a memory area operation unit

managing the key data for dividing to divide the memory area of the integrated circuit to a first memory area

5 wherein at least one of a write operation of data and re-write data in the memory area is authorized on the condition that the first area management key data is used and a second memory area wherein at least one of a write operation of data and a rewrite operation of data in the

10 memory area is authorized on the condition that the second area management key data is used by using the key data for dividing.

26. A method of issuing a portable unit as set forth in claim 25, wherein said portable unit is a card.

15 27. A program for making a computer execute processing so that a portable device mounting an integrated circuit storing key data for dividing, a system code for identifying a first service provider, and first area management key data which is authorized to

20 perform at least one of a write operation of data to a memory area of said integrated circuit and a rewrite operation of data to the memory area on the condition that the first area management key data is used makes a second service provider provide a service using part of

25 said memory area of said integrated circuit when issued

10001000-02200021

by a first service provider providing a first service using said memory area, comprising making the computer execute

a routine for receiving as input the system

5 code from the integrated circuit;

a routine for referring to a registerable

system code list indicating the system code given to the first service provider which can provide a service by the same integrated circuit as the second service provider.

10 and judging whether the input system code is indicated in
the registerable system code list; and

a routine for outputting to the integrated circuit a module including second area management data

15 of the program and encrypted by the memory area operation

unit by using the key data for dividing and further encrypted by the first service provider by using the

first area management key data when judging that the

28. A data processing method for processing so that

distribution key data, a system code for identifying a
signature, a message identifier, and a signature key.

35. data which is authorized to perform at least one of

write operation of data to a memory area of said integrated circuit and a rewrite operation of data to the memory area on the condition that the first area management key data is used makes a second service provider provide a service using part of said memory area of said integrated circuit when issued by a first service provider providing a first service using said memory area, comprising:

10 a routine of inputting the system code from the integrated circuit;

15 a routine of referring to a registerable system code list indicating the system code given to the first service provider which can provide service by the same integrated circuit as the second service provider and judging whether the input system code is indicated in the registerable system code list; and

20 a routine of outputting to the integrated circuit a module including second area management data issued by a memory area operation unit managing execution of the program and encrypted by the memory area operation unit by using the key data for dividing and further encrypted by the first service provider by using the first area management key data when it judges that the input system code is indicated in the registerable system code list.

29. A program for making a computer execute processing for writing file data to a second memory area of an integrated circuit having a first memory area wherein at least one of a write operation and rewrite operation of file data used for providing a first service is authorized on the condition that first area management key data is used and a second memory area wherein at least one of a write operation and rewrite operation of file data used for providing a second service is authorized on the condition that second area management key data is used, comprising making the computer execute a routine of outputting to the integrated circuit file key data which is issued by a second service provider, used at the time of writing the file data in a third memory area, and encrypted by a third area management data when a plurality of third memory areas are defined in the second memory area, a third memory management key data used for performing at least one of a write operation of data to a third memory area and a rewrite operation of data in the third memory area is defined for each of the plurality of third memory areas, and the integrated circuit stores the third area management key data and a routine of writing file data used for providing the second service in the second memory area of

the integrated circuit by using the file key data.

30. A data processing method for performing processing for writing file data to a second memory area of an integrated circuit having a first memory area 5 wherein at least one of a write operation and rewrite operation of file data used for providing a first service is authorized on the condition that first area management key data is used and a second memory area wherein at least one of a write operation and rewrite operation of 10 file data used for providing a second service is authorized on the condition that second area management key data is used, comprising a routine of outputting to the integrated circuit file key data which is issued by a second service 15 provider, used at the time of writing the file data in a third memory area, and encrypted by a third area management data when a plurality of third memory areas are defined in the second memory area, a third memory management key data used for performing at least one of a 20 write operation of data to a third memory area and a rewrite operation of data in the third memory area is defined for each of the plurality of third memory areas, and the integrated circuit stores the third area management key data and 25 a routine of writing file data used for

providing the second service in the second memory area of the integrated circuit by using the file key data.

100134402882